UNITED STATES DISTRICT COURT

for the

District of Oregon

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* A black Hyundai Genesis with Vehicle Identification Number (VIN) KMHGC46F89U058996, as described in Attachment A	Case No. 3:22-mc-146

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

A black Hyundai Genesis with Vehicle Identification Number (VIN) KMHGC46F89U058996, as described in Attachment A as described in Attachment A hereto,

located in the _____ District of Oregon, there is now concealed *(identify the person or describe the property to be seized)*:

The information and items set forth in Attachment B hereto.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2(a) & 2113(a)	Bank Robbery

The application is based on these facts:

See affidavit which is attached hereto and incorporated herein by this reference.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Special Agent Craig Robinson, FBI
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by Telephone at 5:16pm *(specify reliable electronic means)*.

Date: February 9, 2022

Stacie F. Beckerman
Judge's signature

City and state: Portland, Oregon

Hon. Stacie F. Beckerman, United States Magistrate Judge
Printed name and title

DISTRICT OF OREGON, ss: AFFIDAVIT OF CRAIG ROBINSON

Affidavit in Support of an Application Under Rule 41 for a Search Warrant

I, Craig Robinson, being duly sworn, do hereby depose and state as follows:

Introduction and Agent Background

1. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been since March 2020. My current assignment is the Salem Resident Agency in Portland, Oregon Field Office. I have training and experience in federal criminal law and procedure, interview and interrogation techniques, arrest procedures, search and seizure procedures, computer crimes, evidence identification and collection, including electronic evidence. I have personally been involved in matters concerning white collar crimes, violent crimes, illegal narcotics, gun crimes, and the sexual exploitation of children.

2. I submit this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search:

- Black Hyundai Genesis, Vehicle Identification Number (VIN) KMHGC46F89U058996 (hereinafter "**Target Vehicle**"),

as described in Attachment A hereto, for evidence, contraband, fruits, and instrumentalities of the crime of bank robbery, in violation of 18 U.S.C. § 2113(a) (hereinafter the "Target Offense"). As set forth below, I have probable cause to believe that such property and items, as described in Attachment B hereto, including any digital devices or electronic storage media, are currently located inside the **Target Vehicle**.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The facts

set forth in this affidavit are based on my own personal knowledge, knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers, interviews of witnesses, a review of records related to this investigation, communications with others who have knowledge of the events and circumstances described herein, and information gained through my training and experience.

Target Offenses

4. I believe there is probable cause to believe that evidence of the following violations will be found in the vehicle to be searched:

- Title 18 U.S.C. § 2113(a), bank robbery, makes it a felony crime for a person to use force and violence, or intimidation, to knowingly and unlawfully take or attempt to take currency or any other thing of value from a bank or credit union whose deposits are insured by the Federal Deposit Insurance Corporation (FDIC) or National Credit Union Administration (NCUA).

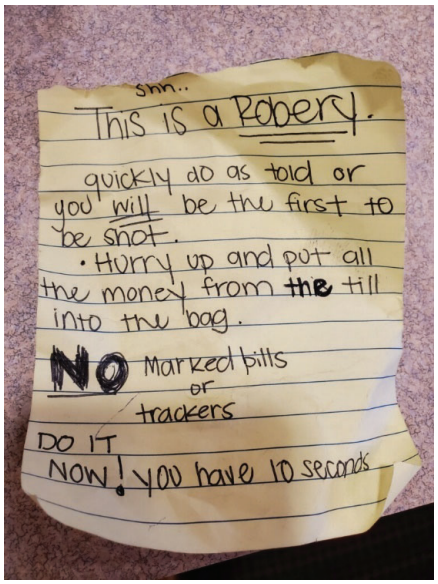
- Title 18 U.S.C. § 2(a), prohibiting a person from aiding, abetting, counseling, commanding, inducing or procuring the commission of an offense against the United States.

Statement of Probable Cause

5. On February 8, 2022, at approximately 3:40 pm, a robbery occurred at the Riverview Community Bank located at 112 Main St, Aumsville, Oregon 97325 (also referred to herein as "the bank"). The bank, whose deposits were then insured by the Federal Deposit Insurance Corporation, suffered a loss of approximately two thousand one hundred ($2,100) in U.S. currency.

6. The victim teller and the bank manager were interviewed by Aumsville Police Chief Rick Schmitz. I spoke with Police Chief Schmitz and he provided the following information:

7. The bank manager and victim teller observed a man, hereafter referred to as "the robber," as he approached the teller station. The robber was wearing a red ball cap, dark colored gaiter around his neck, dark OD green coat, dark shirt, and dark baggy pants. The victim teller reported that the robber appeared to be in his 30s or older, was between 5'10" and 6'0" tall, and he had a little bit of a gut. The victim teller reported the robber handed over a note that said, "This is a robbery. Give me your money with no trackers or you will be the first one shot," and had a black fanny pack with a strap on it. A photograph of the note is below:



8. The robber kept his right hand inside his coat pocket, and the victim teller believed the robber was holding a gun. The victim teller said she was scared and complied with the robbery demand and provided the robber with $2,100 in U.S. currency. The victim teller was still terrified as she relayed the information to Chief Schmitz. She believed the robber had

a gun and she feared for her safety. Chief Schmitz had to calm the victim teller down as he was interviewing her. The bank manager advised that the robber walked briskly out of the bank through the front entrance and east on Main St., over the railroad tracks toward Klein St. The robber was in the bank for less than 5 minutes. The bank manager observed a black sedan parked on Klein St., and she observed the car pull forward as the robber crossed the railroad tracks. The robber entered the passenger door of the black sedan and the car then sped off. I obtained camera footage from inside the Riverview Community Bank from Aumsville Police Department. A copy of the camera footage is below:

///

///

///


4:48
5G
Aumsville2-8-2022
DOCX - 2 MB
Open Word

///

9. The above image depicts a male wearing a red ball cap, dark green coat, black shirt with a white logo on the left side of the chest, dark colored gaiter covering his face, dark baggy pants, and black and white shoes. During the interview of Dustin Halvorsen at the Stayton Police Department, I observed Halvorsen wearing a similar black shirt with a white logo on the left side of the chest and similar black and white shoes as the robber in the attached image.

10. Shortly after the robbery occurred, at approximately 3:49 pm, Marion County Sheriff's Office deputies spotted a black Hyundai Genesis, the **Target Vehicle**, traveling east on Mill Creek Rd. This area is within approximately two miles of the bank that was robbed. It is noted that Klein St. connects to Mill Creek Rd. Marion County deputies ran the license plate on the target vehicle, and the license plate belonged to a truck and not the **Target Vehicle**. Marion County deputies subsequently effected a traffic stop on the **Target Vehicle** as the license plate information did not match the **Target Vehicle**. Marion County deputies observed a male in the passenger seat, and his hands were shaking. The male was later identified by law enforcement as Dustin Halvorsen, with date of birth 07-xx-1984. A female was driving the **Target Vehicle**, and she was being belligerent with Marion County deputies. The female was later identified by law enforcement as Noelle Lerma, with date of birth 02-xx-1999. Deputies did not search the vehicle but were able to see inside the vehicle while standing outside of it. Both Dustin Halvorsen and Noelle Lerma were arrested. Inside the **Target Vehicle**, Marion County deputies observed a red ball cap, along with a dark green coat in the back seat, and a yellow notepad on the back seat. After the **Target Vehicle** was stopped and the occupants arrested, the Aumsville Police sealed up the **Target Vehicle** and towed it to a secure storage

///

facility located at 955 Olney St., Aumsville, Oregon 97325. Photographs of the items observed in the **Target Vehicle** are below:

11. From reviewing the bank's surveillance footage, the red ball cap and dark green coat matched the items worn by the person who robbed the bank. The yellow notepad also matched the same type of paper note used in the robbery. Also observed inside the **Target Vehicle**, and depicted in one of the photographs above, was a cell phone that was seen laying on the floor of the passenger side of the **Target Vehicle**. It is believed that this cell phone belongs to Dustin Halvorsen given that this was where he was sitting inside the vehicle.

Electronic Records

12. As described above and in Attachment B, this application seeks permission to search for records that might be found in the **Target Vehicle**, in whatever form they are found. One form in which the records will likely be found is data stored on digital devices, including cell phones (hereinafter collectively referred to as digital devices). Thus, the warrant applied for would authorize the seizure of electronic storage media or the copying of electronically stored information, all under Rule 41(e)(2)(B).

13. There is probable cause to believe, and I do believe, that records will be stored on a digital device because, based on my knowledge, training, and experience, I know that people who commit crimes with a co-defendant, to include bank robbers and their get-away drivers, have a need to communicate with each other including via phone calls and text messages. I also know that bank robbers will often use the smart phone capabilities of their phones to scout out potential banks to target as well as get-away routes. I also know that:

a. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a digital device, deleted, or viewed via the Internet. Electronic files downloaded to a digital device can be stored for years at little

or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. When a person "deletes" a file on a digital device, the data contained in the file does not actually disappear; rather, that data remains on the digital device until it is overwritten by new data. Therefore, deleted files or remnants of deleted files, may reside in free space or slack space—that is, in space on the digital device that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a digital device's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

b. Wholly apart from user-generated files, digital devices—in particular, internal hard drives—contain electronic evidence of how a digital device has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Digital device users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

c. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

14. As further described in Attachment B, this application seeks permission to locate not only files that might serve as direct evidence of the crimes described on the warrant but also for forensic electronic evidence that establishes how digital devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic

electronic evidence will be on any digital device in the **Target Vehicle**, because, based on my knowledge, training, and experience, I know:

a. Data on the digital device can provide evidence of a file that was once on the digital device but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the digital device that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the digital device was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a digital device can also indicate who has used or controlled it. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, email, email address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the digital device at a relevant time. Further, forensic evidence on a digital device can show how and when it was accessed or used. Such "timeline" information allows the forensic analyst and investigators to understand

the chronological context of access to the digital device, its use, and events relating to the offense under investigation. This "timeline" information may tend to either inculpate or exculpate the user of the digital device. Last, forensic evidence on a digital device may provide relevant insight into the user's state of mind as it relates to the offense under investigation. For example, information on a digital device may indicate the user's motive and intent to commit a crime (e.g., relevant web searches occurring before a crime indicating a plan to commit the same), consciousness of guilt (e.g., running a "wiping program" to destroy evidence on the digital device or password protecting or encrypting such evidence in an effort to conceal it from law enforcement), or knowledge that certain information is stored on a digital device (e.g., logs indicating that the incriminating information was accessed with a particular program).

c. A person with appropriate familiarity with how a digital device works can, after examining this forensic evidence in its proper context, draw conclusions about how digital devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a digital device that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a digital device is evidence may depend on other information stored on the digital device and the application of knowledge about how a digital device behaves. Therefore, contextual

///

information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a digital device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a digital device. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

15. In most cases, a thorough search for information that might be stored on a digital device often requires the seizure of the device and a later, off-site review consistent with the warrant. Generally speaking, imaging or copying is the taking of a complete electronic picture of the digital device's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the digital device and to prevent the loss of the data either from accidental or intentional destruction. This is true because:

a. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a digital device has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine digital devices to obtain evidence. Digital devices can store a large volume of information. Reviewing that information for things described in

///

the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Records sought under this warrant could be stored in a variety of formats that may require off-site reviewing with specialized forensic tools. Similarly, digital devices can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the digital device off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

Nature of Examination

16. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant for which I apply would permit seizing, imaging, or otherwise copying digital devices that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the device or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire device, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

17. The initial examination of the digital device will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time

period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

18. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the digital device do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

19. If an examination is conducted, and the digital device and storage media do not contain any data falling within the ambit of the warrant, the government will return the digital device and storage media to its owner within a reasonable period of time following the search and will seal any image of the computer and storage media, absent further authorization from the Court.

20. If a digital device or storage media contains evidence, fruits, contraband, or is an instrumentality of a crime, the government may retain that computer or storage media as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the computer and storage media and/or the data contained therein.

21. The government will retain a forensic image of the digital device for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to

questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

22. On February 8, 2022, U.S. Magistrate Judge Stacie F. Beckerman signed a criminal complaint charging Dustin Halvorsen and Noelle Lerma with the crime of bank robbery, in violation of 18 U.S.C. §§ 2 and 2113(a).

Conclusion

23. Based on the foregoing, I have probable cause to believe, and I do believe, that Dustin Halvorsen and Noelle Lerma committed the crime of bank robbery, in violation of 18 U.S.C. §§ 2 and 2113(a), and that contraband, evidence, fruits, and instrumentalities of the offense, as described above and in Attachment B, are presently located inside the **Target Vehicle**, which is described above and in Attachment A. I therefore request that the Court issue a warrant authorizing a search of the **Target Vehicle** described in Attachment A for the items listed in Attachment B and the seizure and examination of any such items found.

24. Prior to being submitted to the Court, this affidavit, the accompanying application, and the requested search warrant were all reviewed by Assistant United States

///

///

///

Attorney (AUSA) Scott Kerin. I was informed that it is AUSA Kerin's opinion that the affidavit and application are legally and factually sufficient to establish probable cause to support the issuance of the requested warrant.

By phone pursuant to Fed R. Crim. P. 4.1
Craig Robinson
Special Agent, FBI

Sworn in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone at 5:16 p.m. on February 9, 2022.

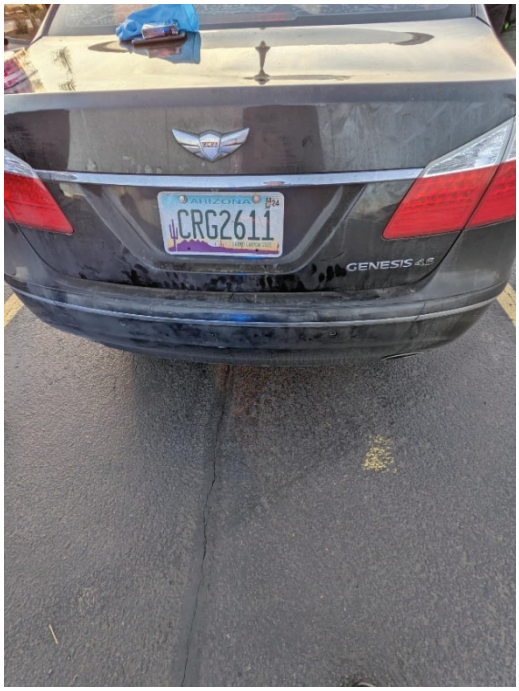
Stacie F. Beckerman

HON. STACIE F. BECKERMAN
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

The property to be searched is a black Hyundai Genesis with Vehicle Identification Number (VIN) KMHGC46F89U058996, located at 955 Olney St., Aumsville, OR 97325. Below are pictures of the vehicle and the VIN:



ATTACHMENT B

Items to Be Seized

The items to be searched for, seized, and examined, are those items inside the **Target Vehicle**, referenced in Attachment A, that contain evidence, contraband, fruits, and instrumentalities of violations of 18 U.S.C. § 2113(a). The items to be seized cover the period of February 8, 2022, through the date of the execution of the search warrant.

1. The items referenced above to be searched for, seized, and examined are as follows:

a. $2,100 cash, to include the following amounts and donations:

1. $1,000 in $50 bills, wrapped in a blank wrapper

2. $100 in $1 bills, wrapped in a blank wrapper

b. Black or dark colored fanny pack with a strap with contents to include above-referenced cash.

c. Red ball cap with an Atlanta Braves logo, matching the red ball cap identified in the camera footage from Riverview Community Bank.

///

///

///

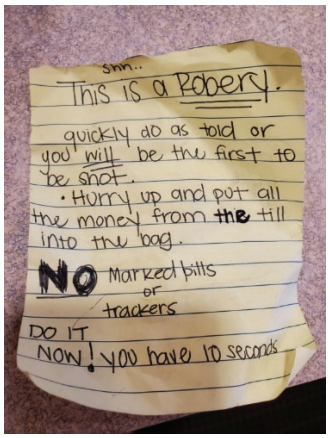

4:48
5G
Aumsville2-8-2022
DOCX - 2 MB
Open Word

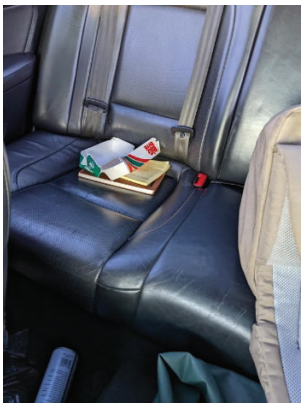
///

///

d. Dark green coat.

e. Notepad with yellow paper, matching the paper used to write the note handed to the victim teller.





f. Papers, records, documents, files, notes, memos, mail, or other materials identifying residencies of Dustin Halvorsen and Noelle Lerma, or ownership or control of target vehicle described in Attachment A.

g. Cellular telephones, computers and other electronic devices capable of storing data that constitutes evidence or the instrumentality of bank robbery.

h. Latent prints and identifying material from items inside the target vehicle.

i. Any firearm or replica of a firearm.

2. As used in this attachment, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware. The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

3. For any electronic devices or storage medium whose seizure is otherwise authorized by this warrant and any computer, storage medium, or digital device that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter "Computer"):

///

a. Evidence of who used, owned, or controlled the digital device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence.

b. Evidence indicating the digital device user's state of mind as it relates to the crime under investigation.

c. Evidence of the attachment to the digital device of other storage devices or similar containers for electronic evidence.

d. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the digital device.

e. Evidence of the times the digital device was used.

f. Passwords, encryption keys, and other access devices that may be necessary to access the digital device.

g. Records of or information about Internet Protocol addresses used by the digital device.

h. Records of or information about the digital device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

i. Contextual information necessary to understand the evidence described in this attachment.

Search Procedure

4. The search for data capable of being read, stored, or interpreted by a computer or storage device, may require authorities to employ techniques, including imaging any computer or storage media and computer-assisted scans and searches of the computers and storage media, that might expose many parts of the computer to human inspection in order to determine whether it constitutes evidence as described by the warrant.

5. The initial examination of the digital device and storage media will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

6. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the computer and storage media do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

7. If an examination is conducted, and the computer and storage media do not contain any data falling within the ambit of the warrant, the government will return the computer

and storage media to its owner within a reasonable period of time following the search and will seal any image of the computer and storage media, absent further authorization from the Court.

8. If a computer or storage media contains evidence, fruits, contraband, or is an instrumentality of a crime, the government may retain that computer or storage media as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the computer and storage media and/or the data contained therein.

9. The government will retain a forensic image of the computer and storage media for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.